VZCZCXRO1125
RR RUEHGA RUEHHA RUEHQU RUEHVC
DE RUEHOT #2158/01 1982020
ZNR UUUUU ZZH
R 172020Z JUL 06
FM AMEMBASSY OTTAWA
TO RUEHC/SECSTATE WASHDC 3177
INFO RUCNCAN/ALL CANADIAN POSTS COLLECTIVE
RUEAHLC/DEPT OF HOMELAND SECURITY WASHDC
RUEATRS/DEPT OF TREASURY WASH DC
RUEAWJA/DEPT OF JUSTICE WASHDC

UNCLAS SECTION 01 OF 03 OTTAWA 002158

SIPDIS

SENSITIVE
SIPDIS

STATE FOR WHA/CAN, EB/IFD/OMA, EB/CBA,
TREASURY FOR IMI:HOEK

E.O. 12958: N/A
TAGS: CA ECON EFIN EAIR ECPS
SUBJECT: CANADIAN VIEWS ON PRIVACY AND TRANS-BORDER
INFORMATION SHARING

REF: A. OTTAWA 2149

¶B. OTTAWA 2060 (NOTAL)

¶1. (SBU) Summary: Canada's Office of the Privacy Commissioner found in a report released June 20 that while the Canada Border Services Agency (CBSA) has systems and procedures in place for managing and sharing personal information with other countries, it needs to improve its management of privacy risks and achieve greater accountability, transparency, and control over the trans-border flow of information (i.e., personal information that is collected or disclosed across international borders). The report is available online at www.privcom.gc.ca. In the past, the federal and provincial privacy commissioners have expressed concern about the protection of personal health data on Canadian citizens which a U.S. corporation may be processing as part of a data services arrangement with a Provincial Health Ministry. More recently, a provincial privacy commissioner has raised concerns about certain medical diagnostic equipment capable of communicating between hospitals. The patient data would travel from Canada through a communication node in the United States back to Canada. Also, a major credit card company recently told the Ambassador that possible future changes to Canada's Anti-Money Laundering and Anti-Terrorist Financing legislation and tighter controls on cross-border data flows could jeopardize much of its Canadian business. End Summary.

Border Services Agency on the Right Track, but Needs Improvement
---

Background

¶3. (U) The Office of the Privacy Commissioner of Canada, which operates independently of the GOC and is mandated by Parliament to act as an ombudsman, advocate, and guardian of privacy rights in Canada, released its annual report on the Privacy Act to Parliament on June 20. The report contained an audit of the "Personal Information Management Practices of the Canada Border Services Agency" that focused on "Trans-border Data Flows."

Reasons for the Audit

¶4. (U) In her report, Privacy Commissioner Jennifer Stoddart pointed to the importance of Canada's exchange of information with the United States as the basis for the audit of the Canada Border Services Agency (CBSA). The CBSA collects personal information about millions of travelers

arriving in Canada that may include detailed financial, family history, and travel information, as well as personal identifiers such as social insurance and passport numbers. Much of this information is retained in an identifiable format either in hard copy (physical files) or in electronic databases.

¶5. (U) The Privacy Commissioner stated a number of reasons for her focus on the flow of information between Canada and the United States. First, the trans-border flow of personal information raises serious inherent privacy risks relating to jurisdictional differences in practices affecting the protection of personal information, the security of personal data in transit, and the adequacy of instruments governing the management of the personal information once it has been shared. Second, there are clear indications that the Canadian public is concerned about the trans-border flow of their personal information to the United States. In a study commissioned by the Privacy Commissioner in 2004, 75% of respondents believed that the Government of Canada transfers Qcitizens' personal information to foreign governments for the purpose of protecting national security, with 85% of those surveyed reporting a moderate or high level of concern about these transfers. In the same vein, many have raised trans-border concerns about data mining, racial profiling, direct access to Canadian databases by the foreign governments (notably the U.S.) and secondary uses of the information. And third, as law enforcement and national security organizations around the world collect more information from more sources about more individuals, and as they use that information to identify possible threats, there is a perceived risk of incomplete or inaccurate data leading to undesirable consequences such as unnecessary scrutiny of individuals.

Privacy Commissioner's Suggestions

¶6. (U) The report found that CBSA has policies, procedures and systems in place for managing and sharing personal information with other countries. However, much can be done to better manage the CBSA's privacy risks and achieve greater accountability and control over personal information that flows across Canada's borders, according to the report:

-- While written requests for assistance from foreign governments seeking CBSA documents are processed in accordance with agency requirements, much of the information shared between the CBSA and the United States at the regional level is verbal, and not based on written requests. This contravenes both CBSA policy requiring the creation of a record when customs information is disclosed and the Canada-United States Customs Mutual Assistance Agreement (CMAA) of June 1984 that requires customs requests for information to be in writing except where pressing circumstances exist.

-- The CBSA needs a coordinated method of identifying and tracking all flows of its trans-border data. The CBSA cannot, with a reasonable degree of certainty, report either on the extent to which it shares personal information with the United States, or how much and how often it shares this information. By extension, it cannot be certain that all information-sharing activities are appropriately managed and that they comply with section 107 of the Customs Act, which provides for protection of customs information and permits the disclosure of customs information to foreign governments and institutions in accordance with a written agreement or arrangement, and section 8 of the Privacy Act, which addresses when personal information under the control of a government institution may be disclosed to, among others, a foreign state.

-- The information technology (IT) and management controls are sound for the Integrated Customs Enforcement System

(ICES) and Passenger Information System (PAXIS). These systems contain sensitive personal information about millions of travelers. Notably, foreign jurisdictions did not have direct access to these systems. Also, electronic releases of information to the United States under the High Risk Travelers and Shared Lookout Initiatives of the CBSA are transmitted over secure communications channels. However, opportunities exist to strengthen the controls to further reduce the risk that personal information could be improperly used or disclosed.

-- The CBSA has not yet evaluated the effectiveness of the High Risk Travelers (HRTI) initiative with the United States because this project has not yet been fully implemented. The Privacy Commissioner recommends that the CBSA assess the extent to which inaccurate or incomplete data may affect individuals or the CBSA's ability to identify, deter, or apprehend "high-risk" travelers. An evaluation would help the CBSA demonstrate that the HRTI initiative has achieved its enforcement and intelligence objectives and, accordingly, that its collection, use and sharing of vast amounts of personal information about millions of travelers are justified.

-- Since the CBSA is a new agency, the time is ripe for it to build and integrate a comprehensive privacy-management framework into its day-to-day information handling practices. In particular, the Privacy Commissioner suggests that the CBSA work toward updating and strengthening the obligations QCBSA work toward updating and strengthening the obligations contained in its personal information sharing agreements with the United States. The CBSA should also consolidate its reporting of privacy incidents and look for ways to improve its mechanisms for monitoring cross-border disclosures of personal information to foreign law-enforcement agencies and other institutions.

-- The Privacy Commissioner recommends that the activities associated with sharing data across borders should be as transparent as possible. A clear and complete picture is not readily available with respect to what information is shared with whom, and for what purpose. As is the case for departments generally, the CBSA does not provide enough detail on the trans-border flows of personal information, or account in a meaningful way for these flows to Parliament and the Canadian public.

Business Concerns on Possible Changes to Canada's Anti-Money Laundering and Anti-Terrorist Financing Laws and on Trans-border Data Flows
---

¶7. (SBU) On June 28, MasterCard Canada CEO Kevin Stanton called on the Ambassador to explain that MasterCard and other large, U.S.-based credit card firms (Capital One, CitiBank, MBNA, Chase and others) are concerned about possible changes to Canada's anti-money laundering and anti-terrorist financing laws. Finance Canada is looking at possible changes, with a view of drafting legislation which could be introduced to Parliament in the fall.

¶8. (SBU) Changes under study include modifications to "know your customer rules" which would require Canadian banks and other financial services firms to better verify the customer's identity when opening a new account or issuing a credit card. According to Stanton, Finance Canada is considering changes that could make portions of MasterCard's current business model unviable in Canada. At present, MasterCard largely issues its credit cards through non-traditional (non face-to-face) means - such as through phone, internet, or direct mail solicitation - rather than through personal applications at bank branches. Such innovations have helped MasterCard to penetrate Canada effectively even though it entered the credit card market

several years after its major competitor, Visa, which issues its credit cards through major Canadian banks. Stanton told the Ambassador that if Canadian credit card applicants in non face-to-face transactions have to take an added step to verify their identity through personally providing officials with a certified copy of a passport, birth certificate, or other document, most will not bother to complete the process due to the inconvenience. MasterCard believes that the GOC should allow the use of reliable third party databases to verify a customer's ID electronically, rather than in person, such as is being done in the UK and the U.S. Stanton argued that this should be an adequate procedure since he did not think that acquiring a credit card presents the same money laundering or terrorist financing risk as opening a bank account, for example.

¶9. (SBU) Moreover, Jennifer Reed, Vice-President of Public Affairs for Mastercard Canada, pointed out in a letter to the Canadian Senate Banking Committee on June 21 that Mastercard already has robust anti-money laundering initiatives in place to deal with their customer financial institutions which subjects the institutions to due diligence reviews. The customer financial institutions must, for instance, have written anti-money laundering programs in place, including appropriate customer identification controls. Reed also wrote that the new legislation would stifle competition by shutting out new competitors and make it significantly more difficult for existing issuers without a branch network to attract new customers.

¶10. (SBU) In his meeting with the Ambassador, Stanton also outlined his firm's concerns about possible tighter Canadian controls on trans-border data flows. This is a concern to MasterCard since virtually all its issuers process and store their credit card data outside Canada, including in the U.S. Stanton said that Canada's 2001 Personal Information Protection and Electronic Documents Act (PIPEDA) will be up QProtection and Electronic Documents Act (PIPEDA) will be up for review shortly, and he is concerned that there could be an effort to place specific restrictions on data going to the U.S., because of an "irrational" fear of U.S. spying. Stanton noted that no one seems concerned about data being stored in other countries, such as India. He said that the federal Privacy Commissioner is under strong pressure from the Canadian Senate to take a tougher line on U.S. data, but claims that she privately wants to resist this with U.S. help.

¶11. (SBU) Post reported in refB public comments on the recent revelations in the U.S. press about the Terrorist Financing Tracking Program.

Visit Canada's Classified Web Site at
http://www.state.sgov.gov/p/wha/ottawa

WILKINS